mation including, but not limited to, medical records. More specifically, the present invention provides a storage location for personal information that stores the information securely and only provides the information to authorized persons to whom the patient has given authority to view and/or use the information, or a subset of the information.

In one embodiment, patients can specify which person or entity may access one's medical information, which portions of the medical information such persons can access, as well as how such information can be viewed. These determinations can be based upon the role or type of entity accessing the information. For example, a research institution can be provided with different aspects of a person's medical information than a doctor. By differentiating access based upon the accessing party's role, anonymous information, for instance, can be provided to a researcher, while a patient's full medical information can be provided to a personal physician. As such, the present invention gives maximum control to the patient and/or eliminates static and potentially out-of-date copies of information from being spread around potentially hundreds of locations.

The present invention permits a patient to access their medical information from any location by establishing a central or distributed repository to which a patient may have their personal information sent and maintained. The main purpose of the repository would be to securely store the medical information and permit only authorized access to the information. The patient would have complete control over the information and those individuals who would be capable of accessing the information. In an emergency situation, however, the present invention contemplates that precertified emergency care providers would be able to override the access limitations to obtain necessary medical information in a manner that would remain highly secure.

In one embodiment, the present invention can utilize a central data repository or a series of repositories that are used to store medical information. A patient would supply their medical information to the repository and request providers to do the same. Each patient would have a universally unique patient identifier. The identifier may be any identifier, such as an alphanumeric sequence, that may then be used to tag each record of the patient's medical information. In another embodiment, the identifier may be recorded on a card with a magnetic strip or on a smart card having a radio frequency identification (RFID) tag with the number stored therein. Still, any of a variety of portable and/or personal storage devices may be used to record such information. In an alternative more secure embodiment, a smart card, such as the RSA SecurID 6100 USB Token, could be used to provide secure mobile patient credentials, or any active security measures, which may include biometrics, private keys, etc.

In any case, the card may be associated with a secret personal identification number (PIN) that is used to control access. The PIN may be a number or may include letters. The PIN may be randomly generated and assigned to the patient or may be specifically chosen by the patient. The PIN may be used to further increase the security over the patient's medical information by ensuring that an unauthorized person could not access medical information simply by using a card.

In alternative embodiments, a patient may obtain additional cards that may be given to family members. As such, in an emergency situation and/or when the patient is not able to access the information themselves, the family member may access the patient's information with the card and, in select embodiments, their own PIN. The PIN may be the patient's PIN or a different PIN. Each provider would be issued their own card and PIN, which permits the system to record which person accessed the patient's medical information, what information was accessed by that person, and limits access to specific content as directed by the patient.

Accordingly, when a patient desires to access their records, they may do so by providing their unique patient identifier, card, and/or PIN to the repository. At that time, the patient has secure access to their records regardless of the location of the patient at any given time.

If the patient wishes to grant access to others, this may be accomplished using a variety of different procedures that safeguard the patient and the patient's information. In one such example, such as when visiting a physician or hospital, the patient would be able to grant access to the physician or hospital by authorizing the physician or hospital to access the patient's records. The doctor's office or hospital would have a reader for reading the patient's card. The reader may be capable of reading magnetic strips, RFID tags, or smart cards, with or without active security features based on biometrics etc. In select embodiments, RFID tags are used with smart cards as RFID tags utilize encryption that is generally more difficult to compromise than magnetic strips. The reader would be specific to the type of media chosen for deployment.

Accordingly, once in the physician's office or hospital, the patient would use their card to identify themselves to the repository Web site. The link to the site may be secured by known means, including, but not limited to, a secured socket layer (SSL) connection, public/private key encryption, or through a virtual private network (VPN). The card and/or PIN would identify the patient to the repository. A cookie or other identifier on a workstation at the physician's office could be used to identify the physician's office and permit the patient to quickly navigate to the correct physician and grant that physician access.

In one embodiment, while the patient is connected, a list of current accessors would also be visible or available to be viewed. The patient could then remove one or more access permissions from their profile on the system thereby keeping the system up to date and/or increasing the security of the patient's information. For example, as access can be granted to parties based upon that parties assigned role, the patient can change the role of an accessor thereby discontinuing that party's privileges. For instance, the role of a physician can be changed from "current medical provider" where the physician has unfettered access to the patient's medical information, to "past medical provider", where the physician has limited or no access to the patient's medical information. Any such changes can alter the access granted to the accessing party including, but not limited to, which items of medical information are available to the accessor, how that information will be viewed, as well as whether the accessor will continue to have access to the patient's medical information at all.

Permitting a physician to have a card and/or PIN would allow the physician to access the patient's records at other times besides those instances when the patient is in the physician's office. For example, the physician would use a single card or mechanism to access medical information for each of that physician's patients. Each patient, being the administrator of his or her own information, would grant the physician access to his or her medical information. The physician, being registered with the present invention and having a PIN and providing that PIN to the system, would then be granted access to the medical information of each patient that granted the physician access.

In one embodiment, the present invention can be configured to require that a PIN be re-entered after a short time out period or period of inactivity, but would be long enough to